Filey Area Primary Schools' Cluster

E-Safety Policy

Our aims are to ensure that all pupils:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use technologies safely.

In order to achieve these goals:

- Pupil's access to content will be subject to age-appropriate filters.
- Pupils will be taught how to effectively use the internet for research purposes.
- Pupils will be taught to evaluate information on the internet.
- Pupils will be taught to recognise online dangers and how to avoid them
- Pupils will be taught how to report inappropriate web content.
- Pupils have opportunities to engage in independent and collaborative learning using the internet and other digital technologies including email.
- Pupils and staff will be provided with individual email accounts. All e-mails are filtered, stored and monitored using Google Vault. Children's email accounts are limited to communication within the school's domain. Emails from outside the domain will only be authorised by the headteacher or e-safety co-ordinator.
- Pupils are not permitted to use mobile phones on the school premises. Such items can be confiscated by school staff if they have reason to think that they are being used to compromise the wellbeing and safety of others (*Education and Inspections Act 2006, Sections 90, 91 and 94)*.

Web Filtering

- The school will work with the Local Authority to ensure that appropriate filtering is in place, using the Local Authority's managed Smoothwall service. In addition, the school will manage filtering both on and off the premises using Google filtering services and the GoGuardian web filtering service.

e-Safety Complaints

- Instances of pupil internet / IT misuse must be reported to a member of staff.
- Sanctions for the misuse of Chromebook technology will reflect those of the current behaviour policy.
- Access to IT resources may be restricted following serious misuse of the technology.
- Staff are trained to deal with e-Safety incidents. They must log incidents reported to them and refer the matter to a senior member of staff. E-Safety issues will be recorded separately on the serious incident log.
- Instances of staff internet misuse should be reported to, and will be dealt with by, the Headteacher.
- Pupils and parents will be informed of the consequences of internet / IT misuse.

Whole-School Responsibilities for Internet Safety

Headteacher

- Ensure that the e-Safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that the Governing Body is informed of e-Safety issues and policies.
- Ensure that appropriate funding is allocated to support e-Safety activities throughout the school.

E safety leader (ideally as part of a wider child protection role)

- Establish and maintain a school-wide e-Safety programme.
- Form a school e-Safety group to review and advise on e-Safety policies.
- Work with the e-Safety group to develop, and review, e-Safety policies and procedures.
- Respond to e-Safety policy breaches in an appropriate and consistent manner.
- Form a school e-Safety management group to review the effectiveness and impact of the policy.
- Establish and maintain a staff professional development programme relating to e-Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body

- Appoint an e-Safety Governor who will ensure that e-Safety is included as part of the regular review of child protection and health and safety policies.
- Support the Headteacher and/or designated e-Safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.

- Ensure that appropriate funding is authorised for e-Safety solutions, training and other activities as recommended by the Headteacher and/or designated e-Safety co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).

Teaching and Support Staff

- Contribute to the development of e-Safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data, ensuring they do not allow computers / browsers to 'remember' passwords which give access to school data / information.
- Develop an awareness of e-Safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include e-Safety regularly in the curriculum.
- Deal with e-Safety issues they become aware of and know when and how to escalate incidents.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school, including the use of Social Media (staff must not make any comment on school related issues via social media)
- Take responsibility for their professional development in this area.

Parents and Carers

- Contribute to the development of e-Safety policies.
- Read acceptable use policies and encourage their children to adhere to them.
- Discuss e-Safety issues with their children, support the school in its e-Safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

Chromebook and Computing - Pupil Agreement

Pupils at Sherburn and Luttons will be given a personal Chromebook to use throughout their time at school. This is to be used as a tool to enhance learning, collaboration and communication. Pupil use of this provision may be both directed and independent. Pupils must, however, agree to use this provision under the following set of guidelines and rules. Pupils who do not follow these rules will have their use of this provision removed other than when under close supervision of a member of staff. More serious offences, including any issues of 'cyber-bullying' or deliberate attempts to harm the school or others' work, will be reported to parents and, if appropriate, outside agencies. All pupils' use of email; saving and creation of documents; photo and video use; and web access will be logged and monitored.

1. Pupils should only use their own Chromebooks and not attempt to log on to, or interfere with other pupils' computers.

2. Pupils must take responsibility for looking after their own Chromebooks - this includes: ensuring that they are stored correctly; charged safely using their own chargers and that they are only used with clean hands.

3. Pupils will never use email or other communication tools to offend, intimidate, exclude or in any way 'bully' others.

4. Pupils should ensure that when the teacher is addressing the class that the Chromebook lid should be lowered so as not to be distracted.

7. Pupils must ensure that when carrying their chromebook they use two hands and walk carefully to their destination.

8. When working collaboratively, pupils must ensure they do not interfere with, delete or alter
others' work unless they are offering constructive feedback. This includes deliberately deleting, amending or editing others' saved work without their, or their teacher's, explicit permission.

9. Pupils must not change any setting on their chromebook without permission from their class teacher or other designated member of staff.

10. Pupils must report any problem, concern or incidents which they feel uncomfortable about, to their class teacher or other member of staff and refrain from sharing personal information about themselves whilst online, as detailed in the school's e-safety input.

12. Pupils must ensure they keep their logon details and passwords a secret and report any concerns regarding others accessing their accounts immediately. Pupils must never try to gain access to others' accounts.

13. Pupils must ensure that any work they submit is their own and refrain from copying another pupil's work or files. Text and images taken directly from another source should credit or reference the original author and adhere to copyright.

14. Pupils must ensure they only ever use appropriate images, videos, text and other media in all their work and use of this technology.

15. Pupils must ensure that the camera on the device is only used to record another individual, or group of people, with their permission.

We want every child at school to enjoy and have a positive experience using the latest technologies to enhance their learning. Following the above rules and guidance will help us to achieve these goals.

Chromebook and Computing - Home / School Agreement

Pupils at Sherburn and Luttons will be given a personal Chromebook to use throughout their time at school. This is to be used as a tool to enhance learning, collaboration and communication. Pupil use of this provision may be both directed and independent. In order to maximise the impact of this resource, children may take their Chromebooks home if they, and their parent / carer, agree to the following.

Pupils who do not follow these rules will have their use of this provision removed. More serious offences, including any issues of 'cyber-bullying' or deliberate attempts to harm the school or others' work, will be reported to parents and, if appropriate, outside agencies. All pupils' use of this resource is monitored, including emails and websites visited.

1. Pupils/parents should ensure they always take care of their Chromebooks, taking every care to avoid damage both when in use and during transit. Chromebooks must be carried to and from school using the provided case.

2. Pupils/parents must never use email or other communication tools to offend, intimidate, exclude or in any direct or indirect way 'bully' others.

3. Pupils/parents must not attempt to install any other software or change any setting on the Chromebooks

4. Pupils/parents must report any damage or errors to school at the earliest opportunity

5. Pupils/parents must report any suspected misuse / offensive material to school at the earliest opportunity

6. Pupils/parents understand that whilst every effort is made to filter inappropriate material, this can not be guaranteed and parents should take appropriate steps to monitor children's internet use.

7. Pupils/parents understand that this initiative may be withdrawn, without notice, should the school feel it needs to do so.

I have read, understood and agree to the Chromebook agreement and would like my child to bring their Chromebook home throughout the week

Pupil name: Class:

Signed (parent / carer):
Date

Acceptable Use of IT Agreement

This agreement is designed to ensure that all members of staff and adults are aware of their responsibilities when using any form of ICT and the related technologies such as email, the internet, social media and mobile devices. Members of staff should consult with the Headteacher, IT subject leader or Chair of Governors for further information and clarification.

Members of staff:

- Must only use the school's email, Internet and intranet and other related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body. Individual employees' Internet and other related technologies will be monitored and logged.
- Must only use approved, secure email systems for any school business.
- Must not browse, download or send material that could be considered offensive, and should report any accidental access of inappropriate materials to their line manager.
- Should not use school information systems or resources (e.g. cameras, laptops, memory devices) for personal purposes without specific permission from the Headteacher.
- Are not permitted to use personal portable media for storage of school related data/images (e.g. USB stick) without the express permission of the Headteacher.
- Must ensure any images of children taken on personal mobile phones are deleted from the phone and images only used for school related purposes.
- Any access to cloud stored information / images on personal devices, is password protected.
- Should ensure that all data is kept secure and is used appropriately, whether in school, taken off school premises, or accessed remotely.
- Should ensure that their use of web technologies, including social networking sites, such as Facebook, Twitter, Instagram, YouTube etc. does not question or bring the school or their professional role into disrepute. Members of staff:
  1. Must not comment in **any** form upon **any** subject related to school. This includes persons (staff, pupils, parents or governors), actions or decisions.
  2. Are advised to consider, and set appropriately, their privacy settings on such sites.
  3. Should consider the appropriateness of images and material posted. Once posted online, a message, photo or video clip can be freely copied, manipulated and circulated and will potentially exist forever.
  4. Should not communicate with pupils, in relation to either school or non school business. Members of staff should only communicate with pupils using official school email.
- Are not permitted to contact or communicate with pupils, parents or conduct school business using personal email addresses or telephones.
- Should not give out their own personal details, such as telephone/mobile number or email address, to pupils.
- Must ensure that all electronic communication with pupils and staff is compatible with their professional role.

All members of staff within the school must agree to follow this policy, and understand that failure to do so may result in disciplinary proceedings in line with the School's Disciplinary Procedure.